

AMENDMENTS TO THE CLAIMS

Claim 16: (Currently amended) In a computer network having at least two computing devices in communication, a method for processing parental control audit data available for access on the network, the method comprising:

in response to receiving a request from an application to log audit data on a first computing device, logging the audit data on the first computing device, the logged audit data being associated with a unique identifier of a restricted user, the request from the application to log audit data including a request to log audit data to a parental control channel from which the logged audit data is periodically transferred to a data repository on the receiving computing device ~~logging the audit data on the first computing device;~~

in response to receiving a second request from an application to log audit data on a second computing device, logging the audit data on the second computing device, the logged audit data being associated with the same restricted user, ~~logging the audit data on the second computing device;~~

aggregating the audit data logged on the first computing device with the audit data logged on the second computing device so that both computing devices contain all of the audit data associated with the restricted user logged on the first and second computing devices; and

in response to one of the computing devices receiving a user request to report all of the audit data contained on the first and second computing devices associated with the same restricted user, reporting the aggregated audit data contained on the computing device receiving the request to the requesting user.

Claim 28: (Currently amended) The method of Claim [[26]] 16, wherein the request from the application to log audit data includes a request to a Windows Shell interface to log the audit data directly into the table in the Windows File System database.